AGENDA ITEM 3b
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF JUNE 30, 2010

Audit (Report Issue Date): HIPAA Security Compliance Review (10/20/06)

Division responsible: Information Security Office

Finding 1.1 Description:
A thorough assessment has not been conducted of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all electronic protected health information. The Information Security Office should conduct this assessment.

Current Status:
COMPLETE. The Information Security Office has implemented a Risk Assessment Management Program (RAMP) to comply with the Health Insurance Portability and Accountability Act stipulation that covered entities must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information.

Finding 3.2 Description:
CalPERS' Data Owners and Custodians Practice is not clear on who should supervise employees and contractors working with electronic protected health information or areas that are outside the data control area. Information Security Office should establish or modify security practices to provide clearer guidelines.

Current Status:
COMPLETE. The Information Security Office has implemented procedures for the authorization and supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Finding 3.9 Description:
CalPERS does not have a security practice that requires timely termination of employees' physical access to locations where electronic protected health information can be accessed. Information Security Office should establish or revise current security practice to define the requirement.

Current Status:
COMPLETE. The Information Security Office maintains that CalPERS has a process for terminating access to electronic protected health information. Management acknowledges that periodic logical and physical access reviews are not performed, but states that it is not currently feasible to implement formal reviews.

Finding 4.3 Description:
CalPERS' User Account Maintenance Practice requires timely modification of user access, however, it does not contain requirements regarding access establishment. Information Security Office should modify the practice to provide clearer guidelines.

Current Status:
COMPLETE. CalPERS has established procedures for establishing, documenting, and modifying a user's right of access. It has not fully implemented procedures for periodic

AGENDA ITEM 3b
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF JUNE 30, 2010

Audit (Report Issue Date): HIPAA Security Compliance Review (10/20/06)
review of a user's right of access. The Information Security Office has concluded that it is not feasible to implement additional procedures under current resource constraints imposed by the PSR project.
Finding 5.2 Description: CalPERS Event Logs Practice requires logging of invalid user authentication attempts and unauthorized attempts to access resources. Information Security Office should incorporate current log-in monitoring practices into security risk analysis and risk mitigation strategy. **Current Status:** COMPLETE. The Information Security Office has considered existing log-in monitoring practices as part of its security risk analysis and risk mitigation strategy. While they recognize that additional log-in monitoring can further mitigate the risk, they decided not to based on the current environment and resource constraints imposed by the PSR project.
Finding 5.3 Description: Information Technology Services uses systems to enforce password standards when feasible. Information Security should incorporate various administrators' current password practices into the security risk analysis and risk mitigation strategy. **Current Status:** COMPLETE. The Information Security Office has implemented password management through the Password Practice. Requirements for strong passwords are enforced through technical controls embedded in information technology infrastructure. The Information Security Office requires all employees to complete security awareness training that includes coverage of password practices and risks, and periodically distributes security bulletins to Information Technology Services Branch managers and supervisors stressing the importance of good password management practice.
Finding 8.3 Description: Security Administration should ensure timely implementation of technical safeguards once the security baselines are established and updated. **Current Status:** COMPLETE. The Information Security Office has performed a risk assessment and baselined the security control framework. Information Security Office management plans to conduct the next HIPAA risk assessment within 6 to 12 months following PSR release, and biennially after that. Information Security Office management has also taken responsibility for the process to ensure timely implementation of technical safeguards.
Finding 8.4 Description: CalPERS' Certification and Accreditation Practice requires that information applications and/or systems must undergo security certification and accreditation to certify that the information is protected. Information Security Office should ensure that this is performed periodically.

AGENDA ITEM 3b
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF JUNE 30, 2010

Audit (Report Issue Date): HIPAA Security Compliance Review (10/20/06)

Current Status:
COMPLETE. The Information Security Office has performed a risk assessment and baselined the security control framework. Information Security Office management plans to conduct the next HIPAA risk assessment within 6 to 12 months following PSR release, and biennially after that. Information Security Office management has also taken responsibility for the process to ensure timely implementation of technical safeguards.

Finding 13.2 Description:
Information Security Office practices do not specifically address media re-use. Media may include removable diskettes used by employees. They should either amend the practices to specifically address media re-use or establish an additional practice.

Current Status:
COMPLETE. The Information Security Office has established formal policy stating that all equipment or removable media that contains confidential or personal information must have the information removed or rendered unreadable before it is transferred to another user or disposed of, and all media that contains confidential or personal information must have the information removed before the media are made available for re-use.

Finding 13.4 Description:
CalPERS' security practices do not specifically require the maintenance of records tracking the movements of hardware and electronic media internally. Information Security Office should determine if this is necessary and then establish or amend security practices as necessary.

Current Status:
COMPLETE. CalPERS is currently maintaining a record of movement of hardware and some electronic media devices. For the remaining electronic media devices, such as thumb drives, the Information Security Office has determined that utilizing encryption on these devices and limiting access to ePHI, as well as providing security awareness and HIPAA training to staff, will mitigate any risk brought on by not tracking the movement of the remaining electronic media.

Finding 13.6 Description:
Current security practices and procedures do not require data backup to be created prior to moving equipment. Information Security Office should establish an appropriate security practice to address the need to require data to be backed up before movement of equipment.

Current Status:
COMPLETE. The Information Security Office reports that whenever hardware is reconfigured, including rare instances where hardware needs to be physically moved, contingency copies of all data and systems are made. In addition, systems identified to contain protected health information are backed nightly, with a minimum retention period of 30 days.

AGENDA ITEM 3b
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF JUNE 30, 2010

Audit (Report Issue Date): HIPAA Security Compliance Review (10/20/06)

Finding 14.3 Description:
CalPERS does not have a security practice that addresses access control during an emergency. Information Security should set forth security requirements that access should be restricted only to those persons that have been granted access rights during an emergency.

Current Status:
COMPLETE. The Information Security Office has documented procedures for obtaining necessary electronic protected health information during an emergency.

Finding 16 Description:
A thorough risk analysis of the technical environment in which all electronic protected health information resides has not been conducted. Upon completion of risk analysis, Information Security should document the controls utilized to mitigate the identified risks to an acceptable level.

Current Status:
COMPLETE. Information Security Office has documented the controls utilized to mitigate the identified risks to an acceptable level and has ensured that the controls are implemented.

Finding 18 Description:
CalPERS has not identified all the locations where electronic protected health information resides, we cannot determine whether current security measures are adequate. Information Security Office should determine whether additional controls are needed to ensure that electronic protected health information is properly protected during transmission.

Current Status:
COMPLETE. The Information Security Office has identified and documented the controls that are in place to ensure that CalPERS' is properly protected during transmission on CalPERS' network.

Division responsible: Information Technology Services Branch

Finding 13.5 Description:
Information Technology Services does not maintain an inventory policy for devices and electronic media. Upon Information Security's completion of security practice regarding tracking of hardware and electronic media, they should amend their policy manual to ensure compliance.

Current Status:
COMPLETE. CalPERS is currently maintaining a record of movement of hardware and some electronic media containing ePHI. For the remaining electronic media, such as thumb drives, the Information Security Office has determined that utilizing encryption on

AGENDA ITEM 3b
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF JUNE 30, 2010

Audit (Report Issue Date): HIPAA Security Compliance Review (10/20/06)

these devices and limiting access to ePHI, as well as providing security awareness and HIPAA training to staff will mitigate any risk brought on by not tracking the movement of the remaining electronic media. Therefore there is no additional action that Information Technology Services needs to take at this time.

Finding 14.2 Description:
Technical support staff using shared accounts to access systems that maintain electronic protected health information do not always obtain an approved variance. Security Administration Services should ensure that all users have a unique identifier. An approved variance should be obtained and documented for all shared IDs.

Current Status:
COMPLETE. Security Administration Services revised user provisioning procedures to require approval of shared accounts by the Information Security Office. Information systems containing electronic protected health information have been validated to assure that shared accounts are approved.

Division responsible: Information Security Office

Finding 1.2 Description:
CalPERS implements security measures to protect information assets housed at CalPERS. Information Security Office should implement required specifications and assess whether each addressable specification is a reasonable safeguard in the environment.

Current Status:
IN PROGRESS. The resolution of this finding relies on the closure of all other HIPAA Security findings. Target Completion Date: December 31, 2011.

Finding 1.4 Description:
CalPERS' Event Logs Practice requires specific security events be logged at key servers. However, the practice does not specify which events must be logged at the system. Information Security Office should develop an Information System Activities Review Practice.

Current Status:
IN PROGRESS. Since PSR will be replacing all but one of the ePHI electronic record sets, the Information Security Office has been engaged with PSR and has assisted in clearly defining HIPAA logging criteria for ePHI electronic record sets. Target Completion Date: December 31, 2011.

Finding 6 Description:
CalPERS' Information Security Incidents Practice defines the events considered to be reportable incidents, however, current security practice and procedures do not adequately specify response efforts. Information Security Office should amend current security practices.

AGENDA ITEM 3b
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF JUNE 30, 2010

Audit (Report Issue Date): HIPAA Security Compliance Review (10/20/06)

Current Status:
IN PROGRESS. Information Security Office is updating the Information Security Incident practice and procedures to ensure consistent management and reporting of security incidents, as well as include more detailed response efforts within the procedures. Target Completion Date: September 30, 2010.

Finding 15.1 Description:
CalPERS' Event Logs Practice does not require a retention period of six years or recording of functions performed. Information Security Office should modify the Event Logs Practice to require the recording and retention requirements.

Current Status:
IN PROGRESS. Since PSR will be replacing all but one of the ePHI electronic record sets, the Information Security Office has been engaged with PSR and has assisted in clearly defining HIPAA logging criteria for ePHI electronic record sets including the six year retention requirement. Target Completion Date: December 31, 2011.

Finding 15.2 Description:
The Document Management System does not log; who viewed imaged documents, when and where the imaged documents are created, printed, exported, or viewed. The Event Logs Practice should be modified to provide clearer guidelines.

Current Status:
IN PROGRESS. Since PSR will be replacing all but one of the ePHI electronic record sets, the Information Security Office has been engaged with PSR and has assisted in clearly defining HIPAA logging criteria for ePHI electronic record sets. Target Completion Date: December 31, 2011.